VERSION
V0.3

Règles pour les interventions à distance sur les systèmes d'information de santé

Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

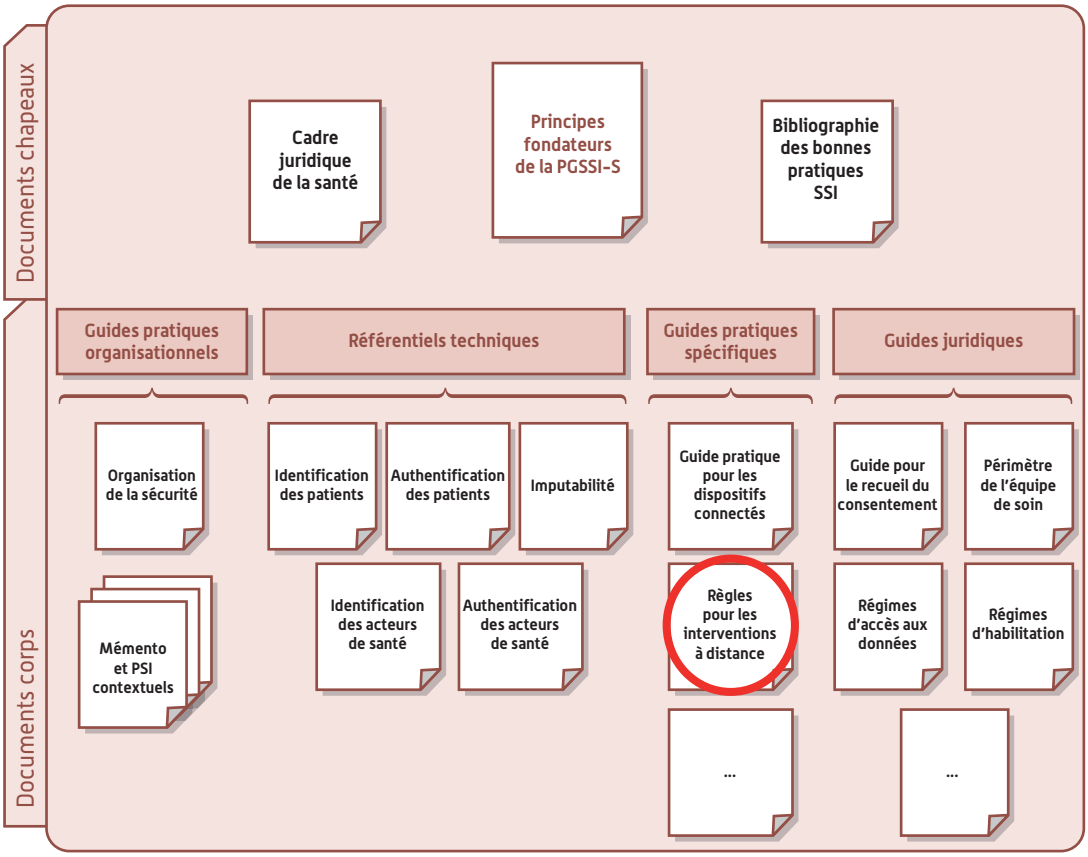
SOMMAIRE

1. INTRODUCTION

1.1. Objet du document

Le présent document définit les règles et les recommandations de sécurité relatives aux interventions effectuées à distance dans un Système d'Information de Santé (SIS).
Il fait partie des guides spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

FIGURE 1 : PLACE DU GUIDE DANS LE CORPUS DOCUMENTAIRE DE LA PGSSI-S



Ce guide spécifique exprime les règles de sécurité auxquelles doivent se conformer, au sein des structures juridiques utilisatrices de SIS, les acteurs responsables de la mise en place et du suivi de prestations effectuées à distance dans les SIS : personnes chargées de la définition, de la contractualisation et du pilotage de ces activités notamment.
Certaines règles sont destinées à être appliquées par les fournisseurs des interventions à distance.

Les règles correspondent aux conditions requises pour que les risques sur la sécurité des informations traitées et sur le fonctionnement d'un SIS restent acceptables lorsque le responsable de ce SIS confie des interventions de télémaintenance, de télésurveillance ou de téléassistance à un prestataire.

Vis-à-vis d'une structure juridique, le fournisseur de prestations à distance peut être un tiers ou une entité interne particulière, par exemple :
- le prestataire informatique d'un professionnel en exercice libéral ou d'un cabinet de groupe ;
- un éditeur de logiciel assurant des prestations de télémaintenance ou téléassistance ;
- l'équipe d'assistance technique rattachée à la DSI d'un établissement de santé ;
- le service support mutualisé mis en place pour le compte de différents SIS.

Le guide s'adresse :

- à la personne responsable de la structure juridique du SIS ainsi qu'aux personnes agissant sous sa responsabilité, notamment :
  - le service achat, pour l'acceptation des engagements du fournisseur à l'égard des règles de sécurité,
  - le responsable de la sécurité du SIS, pour le conseil dans la phase de contractualisation et les questions opérationnelles relatives à la sécurité lors de l'exécution de la prestation,
  - la DSI, pour la mise en œuvre technique et l'exploitation des moyens d'accès distants au SIS,
  - les bénéficiaires de ces activités in fine notamment ceux qui ont des exigences professionnelles de confidentialité, afin qu'ils connaissent les conditions dans lesquelles les interventions sont effectuées ;
- au prestataire auquel est confiée une prestation d'intervention à distance ;
- aux fournisseurs de produits informatiques ou de télécommunication intégrables dans les SIS et pouvant faire l'objet d'interventions à distance.

1.2. Champ d'application du guide

1.2.1. Interventions à distance concernées : la télésurveillance, la télémaintenance, la téléassistance

Dans le cadre de ce guide, les définitions retenues sont :

- La **télésurveillance** est l'activité qui consiste à recueillir à distance et analyser des informations relatives au fonctionnement technique de tout ou partie d'un SIS, en vue de suivre ce fonctionnement, d'en prédire les évolutions ou de détecter d'éventuelles anomalies.
  Exemples : le suivi d'indicateurs de charge d'un ensemble d'équipements, l'exécution cyclique de tests d'une application pour vérifier qu'elle est toujours disponible.

- La **télémaintenance** est l'activité qui consiste à assurer à distance des modifications de paramètres et de configuration de logiciels de tout ou partie d'un SIS afin d'en maintenir le bon fonctionnement ou de faire évoluer son fonctionnement.
  Exemples : l'exploitation et l'administration technique, l'analyse d'incident technique, la mise à jour de logiciel.

- La **téléassistance** est l'activité qui consiste à aider à partir d'un poste distant sur lequel les interfaces d'accès de la personne assistée sont reproduites à l'identique. Dans certains cas la seule interface d'accès reproduite est l'affichage à l'écran et l'intervenant a seulement la possibilité d'observer ce que voit ou fait la personne assistée.
  Exemples : le dépannage logique d'un utilisateur sur son poste de travail, l'apport en direct d'une expertise d'un administrateur sur la console d'un serveur.

L'accès fortuit aux données d'application ou leur accès ponctuel sous le contrôle du bénéficiaire de l'intervention à distance par exemple pour une migration ou une réparation de données, est une éventualité prise en compte dans le document.

Compte tenu de la variété des interventions à distance envisageables, le guide s'applique aux prestations présentant les caractéristiques suivantes.

	Télésurveillance	Télémaintenance	Téléassistance
Le responsable du SIS ne maîtrise pas la sécurité de l'environnement humain, organisationnel, technique ou physique, dans lequel s'exécute la prestation.	***Vrai*** en général Partiellement vrai si le fournisseur appartient à la même structure juridique que le responsable du SIS.		
Le fournisseur a potentiellement accès logique à des informations sensibles du SIS.	***Faux*** en général Les informations techniques surveillées n'ont pas de caractère confidentiel.	***Vrai*** La prestation autorise la connaissance et la modification de données de fonctionnement par le fournisseur (données sensibles en intégrité et parfois en confidentialité). En outre, le personnel du fournisseur peut, même fortuitement, avoir connaissance ou modifier des données applicatives (données de santé par exemple).	
Le fournisseur a potentiellement accès logique à des fonctions sensibles du SIS.	***Vrai*** partiellement Le fournisseur peut activer des tests et agir ainsi sur la disponibilité de fonctions.	***Vrai*** La prestation autorise l'activation, l'arrêt et la modification de certaines fonctions par le fournisseur. Ces privilèges peuvent permettre au personnel du fournisseur d'agir, même fortuitement, sur d'autres fonctions.	
Des moyens informatiques ou de télécommunication spécifiques sont mis en place dans le SIS pour permettre l'intervention à distance.	***Vrai*** L'intervention à distance nécessite des moyens de communication permettant au fournisseur de se connecter à la partie de SIS concernée. En outre, chaque type d'intervention s'appuie sur des outils spécifiques à intégrer dans le SIS.		
Le SIS contient des informations ou des moyens informatiques ou de télécommunication confiés par le fournisseur.	***Possible*** Les moyens mis en place pour permettre l'intervention à distance peuvent provenir du fournisseur.		

1.2.2. Contextes de SIS concernés

Le guide est applicable quels que soient les contextes de SIS rencontrés ou prévus et la structure juridique qui en est responsable, au sens des « Principes fondateurs de la PGSSI-S ».

Le cartouche ci-après présente de manière synthétique le périmètre d'application du document.

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

<u>Limites du champ d'application du référentiel</u> :
Dans ce guide, les interventions à distance n'ont aucune finalité d'opération sur les données d'application, données de santé ou données à caractère personnel notamment. L'hébergement, la sauvegarde, la reconstruction de telles données par exemple sortent du cadre de ce guide.

<u>Plateforme d'intervention à distance :</u>
Dans ce guide, l'évaluation des menaces ainsi que certaines règles font référence au système d'information utilisé par le fournisseur de service pour se connecter sur le système d'information objet de l'intervention à distance. Afin de distinguer ces deux types de système d'information, le système utilisé par le fournisseur est désigné par le terme « plateforme d'intervention à distance » ou « plateforme du fournisseur ».

1.3. Enjeux des interventions à distance

En raison de leurs avantages multiples (efficacité, réduction du délai d'intervention, mutualisation de ressources à forte expertise, …), les interventions à distance sur les systèmes d'information sont aujourd'hui des pratiques courantes.

De telles possibilités d'intervention sur un système d'information supposent la mise en place de moyens spécifiques d'accès à distance et l'attribution de privilèges parfois très élevés au personnel concerné pour pouvoir réaliser les opérations requises. Le responsable du système d'information n'a pas la pleine maîtrise de l'environnement humain, organisationnel, technique et physique dans lequel les prestations à distance sont effectuées.

Ces caractéristiques des interventions à distance introduisent des vulnérabilités supplémentaires dans les systèmes d'information et sont facteurs de risques d'autant plus élevés que les systèmes et leurs informations sont sensibles.

Tel est le cas des SIS. Les données de santé ont de fortes exigences d'intégrité et de confidentialité et certains traitements ont de fortes exigences de disponibilité ou d'auditabilité. Les risques sur la sécurité de ces biens essentiels peuvent être élevés en cas d'accès distant incontrôlé.

En conséquence et afin de répondre à la situation particulière des SIS, les règles édictées dans le présent document visent à permettre en pratique :

- par le responsable d'un SIS, la mise en place de la sécurité organisationnelle et technique nécessaire et la vérification que les risques représentés par l'intervention à distance sont acceptables ;
- par le fournisseur d'une prestation de télésurveillance, de télémaintenance ou de téléassistance, l'expression de son engagement à l'égard de la sécurité des services fournis.

2. FONDEMENTS DU GUIDE

2.1. Documents de référence

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié deux documents couvrant certains aspects des interventions à distance :

- le guide « **Maîtriser les risques de l'infogérance - Externalisation des systèmes d'information** »[1] ;
- la note technique « **Recommandations de sécurité relatives à la télé-assistance** »[2].

Le guide ANSSI couvre les prestations informatiques ou de télécommunication confiées à des tiers, quelle que soit leur nature. Il traite en particulier le cas des prestations effectuées à distance. Pour ces dernières, il indique les vulnérabilités fréquemment rencontrées, souligne les risques principaux d'intrusion et d'abus de privilège d'accès et émet des recommandations.

La note concerne la sécurité de la téléassistance et en particulier de la prise de main à distance sur un poste de travail. Elle précise les risques associés et donne des recommandations minimales à respecter.
Les recommandations de ces deux documents sont reprises dans leurs principes par le présent guide.

2.2. Les menaces induites par les interventions à distance

Le tableau suivant illustre les menaces engendrées par les interventions à distance.

Cas de figure possibles	Menaces à l'encontre du SIS
Le responsable du SIS ne maîtrise pas la sécurité de l'environnement humain dans lequel s'exécute la prestation.	Erreur, négligence, transgression, malveillance ou reniement d'actions du personnel chargé de la prestation, ingénierie sociale à l'égard de ce personnel.
Le responsable du SIS ne maîtrise pas la sécurité de l'environnement organisationnel dans lequel s'exécute la prestation.	Défauts d'exécution ou de qualité de la prestation, conduisant à des indisponibilités du SIS, des pertes de confidentialité ou d'intégrité des données. Divulgation de données de la prestation vers des entités du fournisseur ou des organismes tiers (en cas de sous-traitance notamment), susceptible d'entraîner la violation d'obligations légales ou réglementaires ou l'incapacité çà répondre à des injonctions des institutions judiciaires. Accès logique au SIS par du personnel non autorisé du fournisseur.
Le responsable du SIS ne maîtrise pas la sécurité de l'environnement technique dans lequel s'exécute la prestation.	Propagation d'incidents de sécurité dans le SIS par la plateforme du fournisseur : codes malveillants, attaques logiques de la plateforme. Accès logique illicite à des données du SIS par les utilisateurs de la plateforme.
Le responsable du SIS ne maîtrise pas la sécurité de l'environnement physique dans lequel s'exécute la prestation.	Capture physique de données de la prestation dans l'environnement de la plateforme du fournisseur, observation du personnel, vol de support de stockage. Destruction de la plateforme, entraînant l'incapacité à assurer la prestation.
Le fournisseur a potentiellement accès logique à des informations sensibles du SIS (sauf dans le cas de la télésurveillance).	Divulgation, modification non autorisée de données applicatives (données de santé notamment). Modification non autorisée de données de fonctionnement du SIS, divulgation d'éléments secrets (mots de passe, clés de mécanismes cryptographiques).

[1] http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html
[2] http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-la-tele-assistance.html

Cas de figure possibles	Menaces à l'encontre du SIS
Le fournisseur a potentiellement accès logique à des fonctions sensibles du SIS.	Utilisation ou modification (ou remplacement) non autorisées, perturbation de fonctions du SIS.
Des moyens informatiques ou de télécommunication spécifiques sont mis en place dans le SIS pour permettre l'intervention à distance.	Attaques sur le réseau d'échange entre le SIS et la plateforme technique du fournisseur : capture ou modification de données échangées, perturbation des échanges, attaque de type man in the middle, usurpation d'identité. Dysfonctionnement du SIS ou de l'outillage mis en place pour raison d'incompatibilité technique, infection du SIS par du code malveillant en provenance de l'outillage, exécution de fonctions non documentées par l'outillage, intrusion dans le SIS.

Par ailleurs, le responsable du SIS doit prendre des précautions à l'égard des aspects suivants :

Le SIS contient des informations confiées par le fournisseur.	Protection insuffisante dans le SIS ou son environnement, conduisant à la perte de confidentialité ou d'intégrité d'informations du fournisseur.
Le SIS contient des moyens informatiques ou de télécommunication confiés par le fournisseur.	Détérioration, modification, usage illicite, vol (copie ou non restitution) de moyens du fournisseur.

3. PRINCIPES DE SÉCURITÉ DES INTERVENTIONS À DISTANCE

Compte tenu des menaces, dès la mise en place d'une prestation d'intervention à distance, le responsable du SIS doit se préoccuper des aspects suivants :

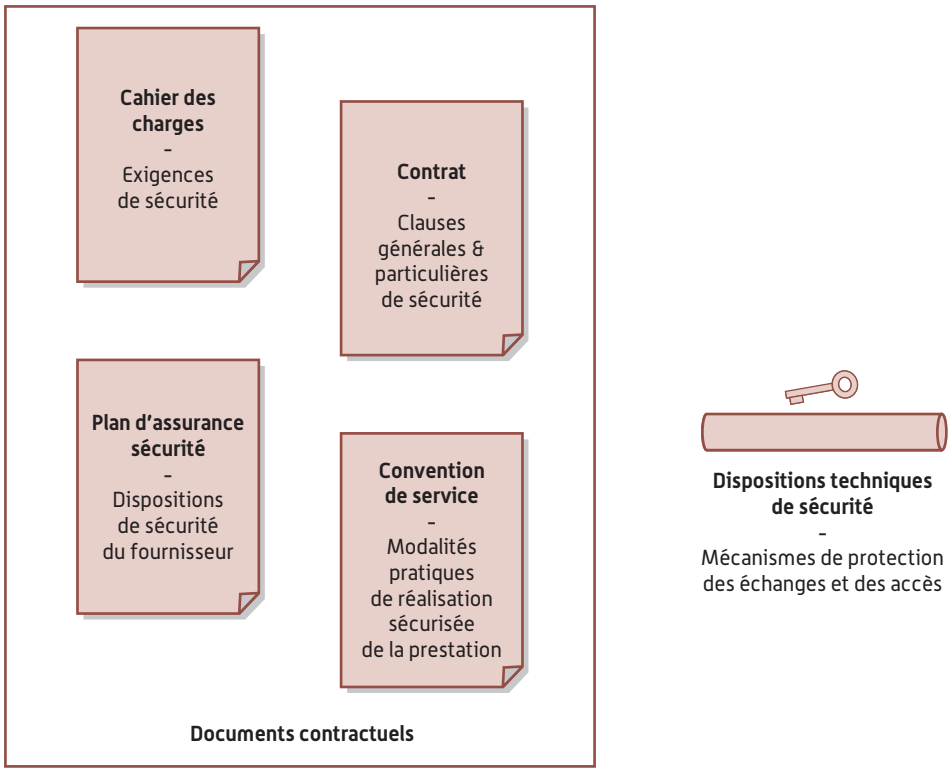
1. La **sécurité de la prestation** elle-même :
   Elle est maîtrisée par le respect des exigences de sécurité du cahier des charges, auquel s'engage le fournisseur au titre d'un contrat.

2. La **sécurité dans l'environnement** humain, organisationnel, technique et physique, **du fournisseur** :
   Elle est maîtrisée par les engagements contractuels du fournisseur, sous forme de clauses générales ou particulières. Les dispositions de sécurité prises par le fournisseur sont décrites dans un plan d'assurance sécurité (PAS) et peuvent être contrôlées par le responsable du SIS.

3. La **protection des échanges et des accès** à distance aux équipements objets de l'intervention.
   Elle est assurée :
   - par des dispositions techniques mises en œuvre au sein du SIS ou entre le SIS et la plateforme d'intervention du fournisseur,
   - par des dispositions organisationnelles décrites dans une « convention de service » intéressant les deux parties et portées à la connaissance des personnes concernées.

En conséquence, la sécurité d'une intervention à distance s'inscrit dans un cadre contractuel, comprenant généralement plusieurs documents applicables du point de vue de la sécurité. Le positionnement de ces documents les uns par rapport aux autres (ex. documents indépendants, différentes annexes du contrat...) n'est pas contrainte du moment que l'ensemble de ces documents sont formalisés et applicables.

FIGURE 2 : ELÉMENTS DE SÉCURITÉ À PRÉVOIR PAR LE RESPONSABLE DU SIS



4. UTILISATION DU GUIDE

Le guide énonce des règles de sécurité dont l'application est du ressort du responsable du SIS.

Le guide impose au responsable du SIS :
- de mettre en œuvre les règles prescrites ou de les faire appliquer par leurs fournisseurs de prestations de télésurveillance, de télémaintenance ou de téléassistance ;
- d'estimer et de traiter les risques de sécurité induits par les règles non appliquées.

Le traitement d'un risque de sécurité peut consister à adopter une ou plusieurs des options suivantes vis-à-vis de ce risque :

- le réduire, par des mesures de protection ou de prévention ;
- l'accepter tel quel notamment si le risque est jugé mineur par le responsable du SIS ;
- l'éviter, par réaménagement de la prestation ;
- le transférer vers un tiers dans le cadre d'un contrat.

L'utilisation du guide s'effectue à partir de la liste des règles du chapitre suivant.

5. RÈGLES DE SÉCURITÉ DES INTERVENTIONS À DISTANCE

Deux paliers sont définis pour la mise en œuvre des exigences de sécurité applicables aux interventions à distance : un palier intermédiaire (Palier 1), porteur des exigences prioritaires, et un palier supérieur (Palier 2) reprenant les exigences prioritaires et les complétant afin d'offrir un meilleur niveau de sécurité.

Les règles applicables au palier 1 sont applicables implicitement au palier 2.

N°	Règle	Applicabilité			Niveau exigibilité
		Télésurveillance	Télémaintenance	Téléassistance	
[C1]	**L'intervention doit être encadrée** par un règlement, un contrat ou une convention entre le responsable du SIS et le fournisseur. Les documents contractuels principaux signés par les parties doivent être fournis en version papier au responsable du SIS. Les autres documents et en particulier les annexes peuvent être mis à disposition via internet sur l'espace client du site du fournisseur.	X	X	X	Palier 1
Des **clauses administratives générales** touchant à la sécurité doivent figurer dans le contrat, précisant les points suivants :					
[C2]	• Le fournisseur est tenu soit d'effectuer toutes les activités de la prestation au sein de l'Union européenne soit de se conformer aux règles définies par la CNIL pour les prestations hors zone de l'Union Européenne[3]. • S'il n'est pas possible de situer ou connaître la localisation des activités (personnel et serveurs informatiques), le fournisseur proposant le service ne peut pas être retenu comme prestataire de service dans ce domaine.	X	X	X	Palier 1
[C3]	• Le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative. Cette déclaration peut être mise à disposition, via internet sur l'espace client du site du fournisseur, associée à une notification des clients par message électronique.	X	X	X	Palier 1
[C4]	• Le fournisseur doit informer, à la signature du contrat, le responsable du SIS de la possibilité d'utilisation de la sous-traitance. À la signature du contrat, le responsable du SIS doit pouvoir indiquer s'il veut que chaque sous-traitance soit soumise à son autorisation ou s'il accepte globalement les sous-traitances que le fournisseur déciderait d'utiliser en cours de contrat. • La liste des sous-traitants utilisés par le fournisseur doit être disponible par exemple via internet sur l'espace client du site du fournisseur.	X	X	X	Palier 2
[C5]	• En cas de recours à la sous-traitance, le fournisseur doit répercuter les exigences qui lui sont applicables vers le sous-traitant.	X	X	X	Palier 1
Des **clauses administratives particulières de sécurité** doivent figurer dans le contrat, précisant que :					
[C6]	• Le fournisseur doit s'engager vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée doit avoir signé un engagement individuel de confidentialité annexé à son contrat de travail.	X	X	X	Palier 1
[C7]	• Le fournisseur doit s'engager vis-à-vis des actions que le personnel peut effectuer. Chaque personne concernée doit avoir signé un engagement individuel de limitation de ses actions au seul besoin des interventions.	X	X	X	Palier 1
[C8]	• S'il le désire, le responsable du SIS a la possibilité de faire réaliser des contrôles des dispositions de sécurité prises par le fournisseur pour la réalisation de sa prestation.	X	X	X	Palier 2

1 http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/

N°	Règle	Applicabilité			Niveau exigibilité
		Télésurveillance	Télémaintenance	Téléassistance	
Des **exigences de sécurité** doivent être imposées au fournisseur par le contrat (clauses techniques ou cahier des charges), précisant les points suivants :					
[E1]	• Le fournisseur doit assurer la sécurité de sa plateforme d'intervention à distance, des points de vue accessibilité, protection des données et des logiciels.	X	X	X	Palier 1
[E2]	• Le fournisseur doit restreindre les accès logiques des postes d'intervention aux seules personnes autorisées. Le fournisseur doit restreindre autant que faire se peut les accès physiques des postes d'intervention aux seules personnes autorisées. A minima, le fournisseur doit sensibiliser les personnes autorisées, à la sécurisation des accès (physiques et logiques) des postes d'intervention et fournir les postes d'intervention et les moyens de sécurité associés.	X	X	X	Palier 1
[E3]	• Le fournisseur doit être en mesure de déterminer en toute circonstance l'identité de toute personne qui se connecte ou s'est connectée sur sa plateforme et en assurer la traçabilité telle que présenté dans les règles [T11] et [T12].	X	X	X	Palier 1
[E4]	Le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la sécurité du SIS ou ses informations ou la sécurité de l'intervention elle-même. Cette exigence concerne : • la lutte contre les incidents de sécurité dans l'environnement humain, organisationnel, technique ou physique du fournisseur et pouvant affecter la sécurité de la prestation fournie ;	X	X	X	Palier 1
[E5]	• la lutte contre les codes malveillants et contre l'exploitation de vulnérabilités connues, dans les moyens informatiques ou de télécommunication mis en place pour la prestation dans le SIS, sous la responsabilité du fournisseur. Par exemple : signaler les vulnérabilités en vue d'une prise de décision commune à leur égard ;	X	X	X	Palier 1
[E6]	• la lutte contre la propagation de codes malveillants ou d'incidents de sécurité à partir de la plateforme du fournisseur, au travers des échanges électroniques effectués au titre de la prestation ;	X	X	X	Palier 1
[E7]	• la lutte contre les codes malveillants dans les logiciels transmis au titre de la prestation ou dans leur mise à jour, et contre l'exploitation de vulnérabilités connues dans ces éléments. Par exemple : signaler les vulnérabilités en vue d'une prise de décision commune à leur égard.		X	X	Palier 1
[E8]	• Le fournisseur doit mettre en œuvre un dispositif de gestion de configuration permettant de contrôler les accès aux composants produits ou fournis au titre de la télémaintenance des logiciels (code source, code exécutable, documentation, données de tests etc…).		X		Palier 1
[E9]	• Le fournisseur doit veiller à ce qu'à l'issue de chaque intervention à distance, les données résiduelles (fichiers temporaires ou zones de mémoire vive) en provenance du SIS soient effacées de la plateforme. Il est à noter que certaines interventions nécessitent plusieurs sessions de connexion sur le SIS (pour des raisons d'investigation par exemple). Une intervention n'est considérée comme terminée que lorsque l'objectif de l'intervention est atteint (résolution d'un incident, mise à jour d'un composant…) ou que le responsable du SIS et le fournisseur déclarent d'un commun accord que l'objectif n'est pas atteignable.	X	X	X	Palier 1

N°	Règle	Applicabilité			Niveau exigibilité
		Télésurveillance	Télémaintenance	Téléassistance	
Le fournisseur doit établir un **plan d'assurance sécurité** (PAS) qui décrit les dispositions de sécurité qu'il met en œuvre pour sa prestation (ou fait référence à une documentation de ces dispositions consultable par le responsable du SIS).					
[A1]	Le PAS peut être un sous-ensemble du plan d'assurance qualité (PAQ). À la signature du contrat, le responsable du SIS doit pouvoir indiquer s'il accepte le PAS type du fournisseur ou si un cycle de validation du PAS est nécessaire. Le PAS fait partie des documents applicables du contrat disponibles via internet sur l'espace client du site du fournisseur. Le PAS doit traiter au minimum les thèmes suivants : • Critères de sécurité utilisés dans la désignation des personnes chargées de l'intervention à distance, engagement de sécurité, information de ces personnes sur la sécurité de la prestation et sensibilisation ; • Règles de protection des informations relatives au SIS ou à l'intervention et détenues par le fournisseur (copie, diffusion, conservation, destruction, transmission) ; • Désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés, séparation vis-à-vis d'autres prestations ; • Architecture générale de la plateforme utilisée pour l'intervention à distance, cloisonnement technique vis-à-vis d'autres prestations, fonctions de sécurité activées dans la plateforme ; • Accès logique des intervenants à la plateforme, identification et authentification, mise en veille et déconnexion automatiques, séparation des tâches, gestion des droits, traçabilité des actions ; • Dispositions prises pour continuer à assurer les activités de la prestation à la suite d'un sinistre majeur ; • Assurance et contrôle de la sécurité des services d'intervention fournis.	**X**	**X**	**X**	**Palier 1**

N°	Règle	Applicabilité			Niveau exigibilité
		Télésurveillance	Télémaintenance	Téléassistance	
Le fournisseur et le responsable du SIS doivent définir les **modalités pratiques** permettant la bonne réalisation de l'intervention à distance (convention de service).					
[01]	Les modalités pratiques doivent être portées à la connaissance des personnes concernées. Elles doivent préciser la prestation en termes de : - objectifs et périmètre ; - obligations réciproques du fournisseur et du responsable du SIS ; - moyens mis en œuvre ; - procédures ; - règles de sécurité. À ce titre, les dispositions organisationnelles de sécurité suivantes doivent être prises en compte :	X	X	X	Palier 1
[02]	• Dans le cas où le responsable du SIS ne pourrait pas fournir une liste actualisée et le numéro de téléphone des personnes pouvant solliciter une intervention à distance, des moyens d'authentification des personnes pouvant solliciter une intervention à distance doivent être définis entre le responsable du SIS et le fournisseur (ex : n° de contrat associé à un mot de passe). • La liste actualisée et le numéro de téléphone des personnes pouvant solliciter une intervention à distance doivent être communiqués au fournisseur pour permettre à son personnel de vérifier la validité des demandes d'intervention.	X	X	X	Palier 2
[03]	• Les interventions de télésurveillance et de télémaintenance doivent être planifiées. Le filtrage de l'accès distant aux équipements concernés ne doit autoriser l'accès que dans les périodes convenues avec les bénéficiaires de ces interventions. Une procédure d'exception peut être prévue pour autoriser temporairement l'accès en dehors de ces plages, afin de répondre à des besoins d'intervention en urgence.	X	X		Palier 2
[04]	• Avant d'accorder l'accès, le bénéficiaire d'une intervention de télémaintenance doit s'assurer des dispositions prises sur la sécurité des données et des traitements à définir au préalable par voie contractuelle. À titre d'exemple : sauvegarde préalable à toute intervention, arrêt de la production, isolement de l'équipement, possibilité de retour arrière en cas d'échec de l'intervention, possibilité de contrôler les opérations effectuées etc.		X		Palier 2
[05]	• Toute intervention de télémaintenance doit faire l'objet d'un rapport transmis à son bénéficiaire par le fournisseur, dans les meilleurs délais. La forme du rapport est à déterminer lors de la signature du contrat entre le responsable du SIS et le fournisseur (document, message électronique de synthèse…) Le mode de transmission du rapport est également à déterminer lors de la signature du contrat (envoi par messagerie électronique, mise à disposition sur l'espace client du site du fournisseur…)		X		Palier 1
[06]	• Les interventions de téléassistance s'effectuent sous le contrôle de leur bénéficiaire. Il appartient à chaque bénéficiaire : - d'autoriser explicitement la prise de main ou le suivi à distance de son poste de travail (affichage d'une demande d'action d'autorisation sur le poste par exemple) ; - d'exiger, s'il le souhaite, de moduler l'accès aux données.			X	Palier 1
[07]	- d'être présent et de suivre les actions distantes sur son poste de travail pendant toute la durée de l'intervention.			X	Palier 2
[08]	• Tout bénéficiaire doit avoir la possibilité technique d'interrompre à tout moment la téléassistance en cours et doit avoir été formé sur la mise en œuvre de cette fonctionnalité.			X	Palier 1

N°	Règle	Applicabilité			Niveau exigibilité
		Télésurveillance	Télémaintenance	Téléassistance	
Le responsable du SIS doit s'assurer de la mise en œuvre des **dispositions techniques de sécurité** suivantes dans le SIS. S'il n'en a pas les capacités techniques, il peut déléguer par contrat la mise en œuvre de ces mesures au fournisseur.					
[T1]	• La connexion directe du télé-mainteneur sur des équipements contenant des applications ou des informations à caractère personnel doit être évitée. • Dans la mesure du possible, un point (ou passerelle) d'accès distant est mis en place pour accéder aux équipements objets de l'intervention à distance. Dans ce cas les règles [T2] à [T5] sont à mettre en œuvre. Dans le cas contraire, les règles [T6] à [T8] s'appliquent :	X	X	X	Palier 1
[T2]	- Les équipements sont reliés à ce point d'accès par un réseau d'administration mis en œuvre soit via un réseau dédié physiquement distinct du reste du SIS, soit via une DMZ ou tout autre mécanisme permettant une isolation logique entre les flux d'administration et le reste du SIS. Cette isolation logique se fera de préférence au moyen d'un VPN.	X	X	X	Palier 1
[T3]	- Le point d'accès distant doit être protégé contre les attaques logiques en provenance des réseaux et son contournement en vue d'accéder au réseau du SIS ne doit pas être possible dans la pratique.	X	X	X	Palier 1
[T4]	- Le point d'accès doit faire l'objet d'audits de sécurité renouvelés destinés à vérifier sa mise en œuvre et sa résistance aux tentatives d'intrusion dans le SIS.	X	X	X	Palier 2
[T5]	- Les échanges entre la plateforme d'intervention et le point d'accès distant au SIS doivent être protégés par des fonctions de chiffrement et d'authentification mutuelle. Ces fonctions sont de préférence conformes au Référentiel Général de Sécurité (RGS).	X	X	X	Palier 2
[T6]	• Si le point d'accès distant n'est pas la solution adoptée, il appartient au responsable du SIS de décider sur recommandation du fournisseur de la solution et du protocole utilisés pour l'échange entre les équipements objets de l'intervention et la plateforme. Dans ce cas :	X	X	X	Palier 1
[T7]	- les échanges doivent être protégés de bout en bout par des fonctions de chiffrement et d'authentification mutuelle ; ces fonctions étant de préférence conformes au Référentiel Général de Sécurité (RGS) ;	X	X	X	Palier 1
[T8]	- un dispositif de filtrage doit autoriser uniquement les flux nécessaires à l'intervention à distance. Ce dispositif peut être à base de filtrage d'adresse IP ou de liste blanche de certificat par exemple.	X	X	X	Palier 1
[T9]	• Chaque équipement objet d'une télésurveillance ou d'une télémaintenance doit disposer d'un compte réservé à cette fin et dont les paramètres d'identification et d'authentification sont différents de ceux de tout autre équipement. Tous les comptes existant par défaut doivent être supprimés ou désactivés, ou leurs paramètres d'identification et d'authentification modifiés.	X	X		Palier 1
[T10]	• En cas d'absence prolongée de trafic dans une session, des mécanismes de surveillance doivent clore automatiquement toute session d'échange établie (en direct ou de part et d'autre du point d'accès) entre la plateforme et un équipement objet de l'intervention. Le délai de déconnexion automatique, à convenir en fonction des caractéristiques de l'intervention à distance, doit être aussi court que possible. Si le responsable du SIS en a la capacité technique, ces mécanismes sont à mettre en œuvre au niveau du SIS. Dans le cas contraire, leur mise en œuvre peut être déléguée par contrat au fournisseur qui les met en œuvre à partir de ses équipements utilisé pour les interventions à distance.	X	X	X	Palier 2
[T11]	• Idéalement, le responsable du SIS doit disposer d'un espace de stockage dans lequel les traces des accès et des opérations effectuées à distance sont centralisées et conservées sous son contrôle, en vue d'être exploitées en cas de litige ou d'incident.	X	X	X	Palier 1
[T12]	• Dans le cas où une centralisation des traces telle que définie dans la règle [T11] n'est pas possible, le stockage des traces peut s'effectuer sur l'équipement objet de l'intervention y compris dans l'espace de l'outillage mis en œuvre.	X		X	Palier 2

6. OFFRE INDUSTRIELLE

Le présent guide décrit une trajectoire d'exigences portant sur l'encadrement des interventions à distance. À ce titre, il permet aux industriels de bâtir leur propre feuille de route de développement de leurs produits et d'afficher de façon formelle la conformité de leurs produits aux paliers exprimés dans le présent document. Selon les paliers, cette conformité pourrait par ailleurs faire l'objet d'une démarche d'homologation telle que préconisée par le RGS.

Ainsi, les responsables de SIS pourront choisir de manière éclairée les prestations d'intervention à distance offrant un niveau de compatibilité clair avec les exigences de la PGSSI-S.

7. IMPACT SUR LES PRATIQUES PROFESSIONNELLES

L'objectif de ce guide spécifique est d'instaurer des mesures de sécurité ayant le moins d'impact possible sur les pratiques professionnelles.

La mise en œuvre initiale des mesures peut avoir un impact marginal sur les pratiques professionnelles dans la mesure où elles nécessitent une configuration des systèmes concernés (ex. indisponibilité des serveurs lors de la mise en œuvre du réseau d'administration tel que présenté dans la règle [T2]). Une fois les mesures mises en place, il n'y a pas d'impact sur les pratiques professionnelles.

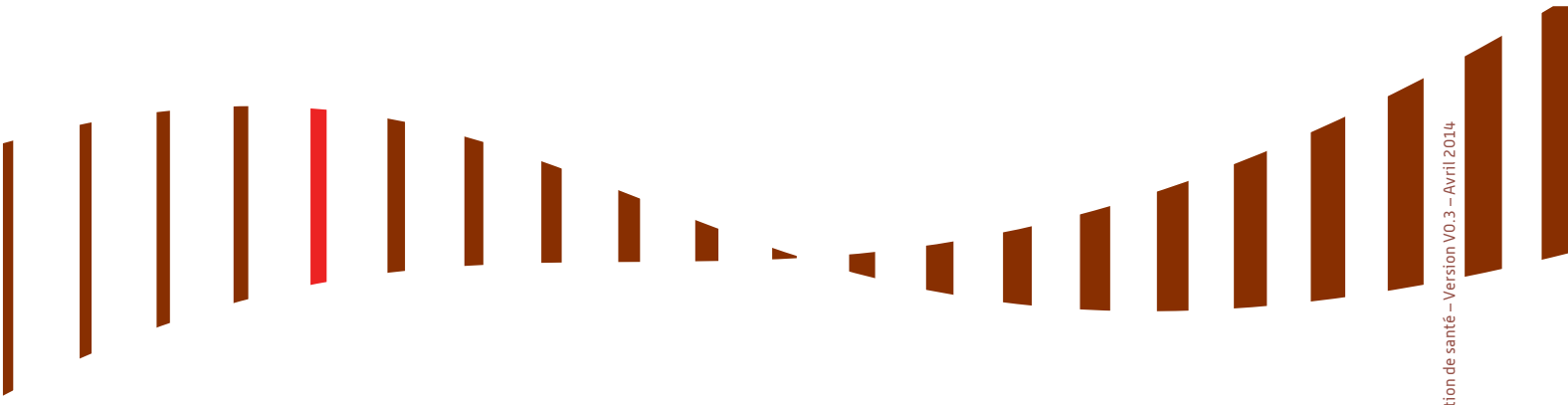
8. ANNEXES

8.1. Annexe 1 : glossaire

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
DSI	Direction des systèmes d'information
PAQ	Plan d'Assurance Qualité
PAS	Plan d'Assurance Sécurité
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
RGS	Référentiel Général de Sécurité
SIS	Systèmes d'Information de Santé
VPN	Virtual Private Network (Réseau privé virtuel)

8.2. Annexe 2 : documents de référence

Référence n° 1 : Externalisation et sécurité des systèmes d'information : maîtriser les risques (ANSSI, 03/12/2010)
Référence n° 2 : Recommandations de sécurité relatives à la télé-assistance (ANSSI, 26/09/2012)



RÉFÉRENTIELS / PGSSI-S – Règles pour les interventions à distance sur les systèmes d'information de santé – Version V0.3 – Avril 2014

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr